What is claimed is:

1. A system for monitoring a network which performs communications based on IP (Internet Protocol), for a cracker attack, comprising:

attack detecting means disposed at a gateway of the network, for successively acquiring IP packets passing through the gateway, storing the acquired IP packets accumulatively, and monitoring the stored IP packets to detect a cracker attack against the network; and

processing means for effecting a predetermined process depending on the detected type of cracker attack when the attack detecting means detects the cracker attack.

2. A system according to claim 1, wherein said attack detecting means comprises means for receiving all IP packets passing through the gateway of the network.

3. A system according to claim 2, wherein said attack detecting means comprises means for receiving only IP packets.

4. A system according to claim 1, wherein said attack detecting means comprises means for holding an algorithm for detecting a plurality of different types of cracker attacks, and detecting the types of cracker attacks from the IP packets acquired and stored by the attack detecting means based on said algorithm.

5. A system according to claim 4, wherein said attack detecting means comprises means for classifying a plurality of the IP packets acquired and stored by the attack detecting means according to at least source IP addresses and/or destination IP addresses, and detecting the types of cracker attacks from the classified IP packets.

6. A system according to claim 1, wherein said attack detecting means comprises means for detecting a cracker attack of a first type when the IP packets acquired and stored by the attack detecting means include at least a predetermined number of IP packets which are transmitted to the network from an external network within a predetermined time, and whose at least source IP addresses are the same as each other, and whose destination IP addresses or destination port numbers are different from each other.

7. A system according to claim 1, wherein said attack detecting means comprises means for detecting a cracker attack of a second type when the IP packets acquired and stored by the attack detecting means include at least a predetermined number of Syn IP packets based on TCP (Transmission Control Protocol), which are transmitted to the network from an external network within a predetermined time, and whose at least destination IP addresses are the same as each other, and when an Ack IP packet based on the TCP which has the same

source IP address and destination IP address as each of the Syn IP packets is not acquired within said predetermined time.

8. A system according to claim 1, wherein said attack detecting means comprises means for detecting a cracker attack of a second type when the IP packets acquired and stored by the attack detecting means include at least a predetermined number of Syn/Ack IP packets based on TCP (Transmission Control Protocol), which are transmitted to the network from an external network within a predetermined time, and whose at least destination IP addresses are the same as each other, and when an Ack IP packet based on the TCP which has the same source IP address and destination IP address as the source IP address and destination IP address of each of said Syn/Ack IP packets is not acquired within the predetermined time.

9. A system according to claim 1, wherein said attack detecting means comprises means for detecting a cracker attack of a third type when the IP packets acquired and stored by the attack detecting means include at least a predetermined number of same divisions of an IP packet, which are transmitted to the network from an external network.

10. A system according to claim 1, wherein said attack detecting means comprises means for detecting a cracker attack of a fourth type when the IP packets acquired and stored by the attack detecting means include at least a predetermined

number of IP packets, which are transmitted to the network from an external network within a predetermined time, and whose source IP addresses are the same as destination IP addresses thereof.

11. A system according to claim 1, wherein said attack detecting means comprises means for detecting a cracker attack of a fifth type when the IP packets acquired and stored by the attack detecting means include at least a predetermined number of IP packets, which are transmitted to the network from an external network within a predetermined time in order to operate a host in the network, and whose user name data of the host are the same as each other and whose passwords of the host are different from each other.

12. A system according to claim 1, wherein said attack detecting means comprises means for detecting a cracker attack of a sixth type when the IP packets acquired and stored by the attack detecting means include an IP packet which has a data sequence having a predetermined pattern of data for attacking a buffer overflow security hole.

13. A system according to claim 1, wherein said processing means comprises means for generating a report output representing the detection of the cracker attack in the predetermined process.

14. A system according to claim 1, wherein said processing means comprises means for preventing an IP packet having a source IP address and/or a destination IP address associated with the attack detected by the attack detecting means, from entering the network in the predetermined process, for a predetermined time after the attack detecting means detects the attack.

15. A system according to claim 6, wherein said processing means comprises means for preventing an IP packet having the same source IP address as the source IP addresses associated with the attack of the first type detected by the attack detecting means, from entering the network for a predetermined time after the attack detecting means detects the attack of the first type, in the predetermined process.

16. A system according to claim 7, wherein said processing means comprises means for preventing an IP packet having the same destination IP address as each said Syn IP packet from entering said network for a predetermined time after said attack detecting means detects the attack of the second type, in said predetermined process.

17. A system according to claim 16, wherein said processing means comprises means for preventing an IP packet having the same source IP address as each said Syn IP packet from entering said network for a predetermined time after said

attack detecting means detects the attack of the second type, in said predetermined process.

18. A system according to claim 17, wherein said predetermined time for which an IP packet having the same source IP address as each said Syn IP packet is prevented from entering said network is longer than said predetermined time for which an IP packet having the same destination IP address as each said Syn IP packet is prevented from entering said network.

19. A system according to claim 8, wherein said processing means comprises means for preventing an IP packet having the same destination IP address as the source IP address of each said Syn/Ack IP packet from entering said network for a predetermined time after said attack detecting means detects the attack of the second type, in said predetermined process.

20. A system according to claim 19, wherein said processing means comprises means for preventing an IP packet having the same source IP address as the destination IP address of each said Syn/Ack IP packet from entering said network for a predetermined time after said attack detecting means detects the attack of the second type, in said predetermined process.

21. A system according to claim 20, wherein said predetermined time for which an IP packet having the same

source IP address as the destination IP address of each said Syn/Ack IP packet is prevented from entering said network is longer than said predetermined time for which an IP packet having the same destination IP address as the source IP address of each said Syn/Ack IP packet is prevented from entering said network.

22. A system according to claim 9, wherein said processing means comprises means for preventing an IP packet having the same destination IP address as the destination IP address of each said divided IP packet from entering said network for a predetermined time after said attack detecting means detects the attack of the third type, in said predetermined process.

23. A system according to claim 22, wherein said processing means comprises means for preventing an IP packet having the same source IP address as the source IP address of each said divided IP packet from entering said network for a predetermined time after said attack detecting means detects the attack of the third type, in said predetermined process.

24. A system according to claim 23, wherein said predetermined time for which an IP packet having the same source IP address as the source IP address of each said divided IP packet is prevented from entering said network is longer than the predetermined time for which an IP packet having the

same destination IP address as the destination IP address of each the divided IP packet is prevented from entering said network.

25. A system according to claim 10, wherein said processing means comprises means for preventing an IP packet having the same source IP address and destination IP address as each of the IP packets associated with the attack of the fourth type from entering the network for a predetermined time after the attack detecting means detects the attack of the fourth type, in the predetermined process.

26. A system according to claim 11, wherein said processing means comprises means for preventing an IP packet having the same source IP address and destination IP address as each said IP packet associated with the attack of the fifth type from entering said network for a predetermined time after said attack detecting means detects the attack of the fifth type, in the predetermined process.

27. A system according to claim 12, wherein said processing means comprises means for preventing an IP packet having the same source IP address and destination IP address as the IP packet associated with the attack of the sixth type from entering the network for a predetermined time after the attack detecting means detects the attack of the sixth type, in the predetermined process.

28. A system for monitoring a network which performs communications based on IP (Internet Protocol), for a cracker attack, comprising:

attack detecting means disposed at a gateway of the network, for successively acquiring IP packets passing through the gateway, storing the acquired IP packets accumulatively, holding an algorithm for detecting a plurality of different types of cracker attacks, and monitoring to detect the types of cracker attacks from the acquired and stored IP packets based on the algorithm; and

processing means for preventing an IP packet having a source IP address and/or a destination IP address associated with the attack detected by the attack detecting means, from entering the network according to a predetermined process, for a time which is predetermined corresponding to the detected type of attack, after the attack detecting means detects one of the attacks.

29. A system according to any one of claims 14 through 28, further comprising a packet filter disposed at the gateway of the network, for selectively establishing IP packets to be prevented from entering the network, the processing means comprising means for controlling the packet filter to perform the predetermined process.